

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the
Northern District of New York

In the Matter of the Search of)

(Briefly describe the property to be searched or identify the person by
name and address))ONE SILVER APPLE IPHONE, CURRENTLY
LOCATED AT A SECURE FACILITY IN LATHAM,
NEW YORK)

Case No. 1:24-mj- 567(DJS)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 2423(b)

Offense Description

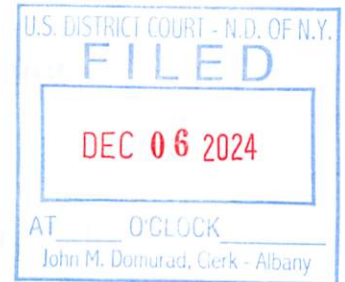
(travel with intent to engage in illicit sexual conduct)

The application is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



John F. Montesano Jr. 4312
Applicant's signature

John F. Montesano Jr., FBI TFO

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ (specify reliable electronic means).

Date: December 6, 2024

City and state: Albany, New York

Hon. Daniel J. Stewart
Judge's signature
Hon. Daniel J. Stewart, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A
SILVER IPHONE, CURRENTLY LOCATED
AT A SECURE FACILITY IN LATHAM,
NEW YORK

Case No. 1:24-MJ-

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, **JOHN F. MONTESANO**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer (“TFO”) with the Federal Bureau of Investigations (“FBI”) and Investigator with the New York State Police (“NYSP”). My assignments include investigating violations of federal law – specifically, violent criminal offenses against children, including those involving sexual exploitation of children. I am currently investigating federal violations concerning the sexual exploitation of children and the sexual trafficking of children. I have also attended and completed trainings, seminars, and classes covering such crimes and investigations.

3. I am an investigative or law enforcement officer of the United States within the meaning of Title 18 United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses

enumerated in Title 18, United States Code. Section 2516(1). As an FBI/TFO, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including the offenses described herein.

4. I am currently investigating DAVID GRUBER ("GRUBER") for traveling in interstate commerce with intent to engage in any illicit sexual conduct with another person, in violation of 18 U.S.C. § 2423(b); that is: mouth to vagina and penis to vagina contact with a 9-year-old female child, sexual acts as defined in Title 18, United States Code, Section 2246, with a person under 18 years of age that would be in violation of Chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction of the United States, that is: Aggravated Sexual Abuse in violation of 18 U.S.C. § 2241(c). (the "Subject Offense"). This affidavit is submitted in support of a search warrant to search a silver iPhone, an electronic device, which was taken off the person of GRUBER at the time of his arrest (hereinafter, the "Device")

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Because this Affidavit is being submitting for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses are located in the Subject Device.

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images.

This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected

to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

7. Based on my training, experience, and research, the Device appears to be a "smart phone" which has capabilities that allows it to serve as **a wireless telephone, digital camera, portable media player, GPS navigation device, PDAs and access the internet.** In my training

and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

DEFINITIONS

8. The following additional definitions apply to this affidavit and Attachments A-B:
 - a. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
 - b. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1)
 - c. “Visual depictions” includes undeveloped film and videotape, as well as data stored on computer disk or by electronic means, which is capable of conversion to visual image. *See* 18 U.S.C. § 2256(5)
 - d. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic

or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs, memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital files and printouts or readouts from any magnetic, electrical or electronic storage.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

9. The property to be searched is a silver iPhone recovered from David Gruber's person on December 5, 2024 (hereinafter the "Device") The Device is currently located at an evidence locker in Latham, New York

10. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

BACKGROUND OF THE INVESTIGATION

11. On or about November 28, 2024, an FBI Task Force Officer, acting in an undercover capacity ("UC1"), created an online persona as a male with access to a nine-year-old girl on a social networking application for people interested in sexual fetishes. ("Application 1"). Application 1 is a free mobile messaging application that allows people to communicate in both public chat rooms and through direct messaging between two or more users. UC1's display name on Application 1 was "princesspeachmk" GRUBER initiated a conversation with UC1 in the chatroom "famfun."

12. On November 28, 2024, GRUBER, using screenname “wheresdaffillin88” initiated a private conversation with UC1 on Application 1 about arranging a meeting with UC1’s “family friend’s daughter” to perform illicit sexual acts.

Sender	Message
wheresdaffillin88	39m pa- asl 🤗 fam room
UC1	42. M. Upstate NY
wheresdaffillin88	Oh cool man not far then. How olds your daughter.
UC1	Very Young
wheresdaffillin88	Oh yeah? Sharing?
UC1	In person. Yes

During the conversation, UC1 explained to the GRUBER that he has access to “a family friend’s daughter” but needed to pay the mother each time he took the girl. The GRUBER replied stating “when you get her – you can instruct us both what to do” and “Jesus I just got so hard thinking about this.”

13. On November 29, 2024 at 6:55 am GRUBER messaged UC1 to discuss downloading an encrypted messaging application (“Application 2”) in order to continue the conversation in a more private application. After discussing the application, which UC1 did not download, GRUBER told UC1 which sexual acts he intended to perform on the child stating he would “eat her pussy, have her suck [his] cock, then fuck.” When UC1 stated the girl was nine-years-old, the GRUBER responded “Oh damn for real a young one.” Later in the day, UC1 stated the nine-year-old’s mother would need a “couple hundred” dollars for UC1 to get access to the nine-year-old. GRUBER responded “I got it. Don’t worry. Ill pay her.” When GRUBER asked where the meet up would take place, UC1 responded it would at his home or camper near Albany, New York.

14. On November 30, 2024, GRUBER asked for a photo of the nine-year-old girl giving the peace sign. UC1 sent GRUBER an age-regressed photograph of a female law enforcement agent which appeared to be a 9-year-old girl holding up 2 fingers. UC1 then sent three additional pictures digitally altered to look like the same nine-year-old girl. GRUBER responded stating: "Wow... smokin hot man." GRUBER further described what sexual acts he would perform on the nine-year-old explaining that due to the size of his penis he would need to "go slow" and he definitely would "not [get] it all in." When UC1 described the nine-year-old girl's vagina as "bald and tight" GRUBER replied "fuck yeah man. Damn you got me excited lol."

15. On December 2, 2024, GRUBER negotiated with UC1 a price to pay the nine-year-old's mother so that GRUBER could perform sex acts on the nine-year-old. UC1 messaged that the mother "wants like 200 dollars to take her daughter" and the target replied "I told you I got cash. Will she take say 250 when you take her home?" When UC1 said he was trying to figure things out, GRUBER said "offer her \$300 then but that's after you drop her off." UC1 relayed that the mother "said I can have her on Thursday. Just gotta pay her after."

16. Throughout the messages between GRUBER and UC1, GRUBER emphasized on multiple occasions to UC1 that he was serious, that UC1 "got [his] guy;" and that GRUBER hoped UC1 was "serious too."

17. GRUBER suggested that he meet UC1 and the nine-year-old girl on either Wednesday, December 4 or Thursday, December 5. and GRUBER and UC1 agreed to meet around 6:00 p.m. on December 5 in an apartment building in Albany County, New York. GRUBER stated that he would drive from Pennsylvania to Albany County that day and would send pictures of himself driving to the location.

18. On December 5, 2024, GRUBER sent pictures of exit signs from his vehicle while driving from Pennsylvania to Albany County, New York, including an exit sign for downtown Trenton, a New Jersey city just across the Pennsylvania border. License plate reader ("LPR") photographs captured GRUBER's car in New Jersey and New York as he drove to Albany County. While driving, GRUBER messaged UCI again about the sexual acts he intended to perform on the nine-year-old girl asking, "And you told her to suck and fuck me?" and "Did you pop her cherry? I think I'm only gonna go half in."

19. At approximately 9:00PM on December 5, 2024, GRUBER arrived to meet the nine-year-old girl at a prearranged location in Albany, County. GRUBER was confronted by law enforcement upon arrival. GRUBER was observed driving the same vehicle captured on the LPR photographs described above.

20. Law enforcement recovered the Device from Gruber's person incident to his arrest

21. In a *Mirandized* interview, GRUBER stated in substance that he drove from Pennsylvania to Albany County to have sex with someone he knew to be a child. GRUBER also acknowledged that he sent the messages from username "wheresdafillin88" to UCI.

22. The acts GRUBER intended to perform on the nine-year-old personal, as set for the above, would constitute, among others, the following crimes under New York State Penal Law:

- a. New York State Penal Law § 130.50, Criminal Sexual Act in the First Degree;
and
- b. New York State Penal Law § 130.35, Rape in the First Degree.

23. The Device is currently in storage in Latham, New York. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Your Affiant is trained in computer and cellular telephone evidence recovery and has extensive knowledge about the operation of cellular telephones and computer systems including the correct procedures for the seizure and analysis of these systems.

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

27. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active

file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

28. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

29. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

FORENSIC ANALYSIS

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.


31. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion

onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. Based upon the above information, there is probable cause to believe that evidence of a violation of the Subject Offense, as outlined in Attachment B of this Affidavit, will be found within the Device. Therefore, your Affiant requests the Court issue the attached search warrant authorizing the search of the Device, a silver iPhone, which was taken off the person David Gruber at the time of his arrest, as described in Attachment A, for the items more particularly described in Attachment B.

Respectfully submitted,

 # 3120

John F. Montesano
Task Force Officer
Federal Bureau of Investigations

I, the Honorable Daniel J. Stewart, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on December 6, 2024, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Subscribed and sworn to before me
on December 6, 2024:



Honorable Daniel J. Stewart
United States Magistrate Judge

ATTACHMENT A

The property to be searched is the Device, as described below:

- a. A silver iPhone, which was taken off the person of David Gruber at the time of his arrest, and is currently in the possession of the FBI in the Northern District of New York

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEARCHED AND SEIZED

Items and information that constitute fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2423(b) (traveling in interstate commerce for the purpose of engaging in illicit sexual conduct with another person, such conduct being a sexual act with a person under 18 years of age), described as follows:

- a. Documents and records regarding the ownership and/or possession of the Device
- b. Electronic data to include deleted data, remnant data, and slack space
- c. Documentation that explains the configuration or use of the Device
- d. Passwords, and programs, or data that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any electronic data records.
- e. Personal and business documents, monthly statements, payment history, and carrier invoices regarding the ownership and/or possession of the Device.
- f. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history to determine the chronological context of the cellular device use, account access, and events relating to the crimes under investigation.

g. Records, documents, correspondence, notes and/or other materials relating to the correspondence or contact between the undercover (UC1) and Gruber, to include images and videos sent to UC1 and images sent by UC1.

h. Records, documents, correspondence (including but not limited to electronic communications), notes, and/or any other materials relating to correspondence or contact between the defendant and individuals purporting to be mirrors, or any attempt to by the defendant induce any minor to engage in illegal sexual activity.

i. Evidence of use of social media applications, including the user attribution, used to communicate with UC1

2. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.